A Structure Theorem for Some Matrix Algebras

Thomas J. Laffey
Department of Mathematics
University College
Dublin 4, Ireland

Submitted by F. Uhlig

ABSTRACT

Let F be a field, and $M_n(F)$ the algebra of $n \times n$ matrices over F. It is in general a very difficult and tedious problem to determine the structure of the subalgebra X of $M_n(F)$ generated by a given subset S of $M_n(F)$. We show that if X contains a matrix A with n distinct eigenvalues in F, then X can be determined up to similarity very quickly by a graph-theoretic method. As a consequence we show that any such X can be generated by a pair of elements one of which can be taken to be A and the other a $(0,1)$ matrix. As an application, we obtain a Specht-type similarity theorem.

Let S be a nonempty set of $n \times n$ matrices. Define the directed graph $G(S)$ of S as follows: $G(S)$ has vertices $1, 2, \dots, n$; vertices i, j are joined by a directed edge if and only if there exists $B = (b_{st}) \in S$ with $b_{ij} \neq 0$. [Thus $G(S)$ is the graph of the "generating matrix" $\sum_{B \in S} x_B B$, where the x_B are distinct indeterminates, in the usual sense.]

We write $i \to j$ to denote that i, j are path-connected, i.e., there exist $r \geqslant 1$ and $i_1 = i, i_2, \dots, i_r = j$ such that $i_1 i_2, i_2 i_3, \dots, i_{r-1} i_r$ are edges in $G(S)$, i.e., for each $k = 1, 2, \dots, r-1$, there exists $B_k \in S$ such that $b^{(k)}_{i_k i_{k+1}} \neq 0$, where $B_k = (b^{(k)}_{uv})$. We write $i \leftrightarrow j$ if either $i = j$ or $i \to j$ and $j \to i$. Note that $\leftrightarrow$ is an equivalence relation on $G(S)$. We denote by $[i]$ the $\leftrightarrow$-equivalence class of i.

The $\leftrightarrow$-equivalence classes are called the *strongly connected components* or *strong components* of $G(S)$.

Given two distinct strong components $[i], [j]$, we write $[i] \to [j]$ if there exist $u \in [i]$, $v \in [j]$ with $u \to v$. We say that a strong component $[i]$ is a *terminus* if $[i] \not\to [j]$ for any strong component $[j] \neq [i]$. Note that if $[i], [j]$

655 Avenue of the Americas, New York, NY 10010 0024-3795/92/$5.00

are distinct strong components, then at most one of the statements $[i] \to [j]$, $[j] \to [i]$ is true. It follows that termini exist. In the book of Behzad, Chartrand, and Lesniak-Foster [3], the condensation of a directed graph is formed by shrinking each strong component to a single vertex; they prove that the resulting graph is acyclic and hence has a vertex of outdegree zero (i.e. a terminus in our terminology).

We can order the set $[G(S)] = \{[v_1], [v_2], \dots, [v_r]\}$ of strong components so that $[v_1]$ is a terminus, $[v_2]$ is a terminus of $[G(S)] - \{[v_1]\}$, v_3 is a terminus of $[G(S)] - \{[v_1], [v_2]\}$, etc. Note then that $[v_i] \nrightarrow [v_j]$ if $j > i$.

Let G be a directed graph on n vertices with strong components $[v_1], [v_2], \dots, [v_r]$ of sizes $k_1, k_2, \dots, k_r$, respectively. Let B be an $n \times n$ matrix partitioned into r^2 blocks B_{ij} where B_{ij} is of size $k_i \times k_j$. Then we shall say that the matrix B is of type G if

$$B_{st} = 0 \quad \text{whenever} \quad [v_s] \nrightarrow [v_t].$$

Notice that if the strong components have been ordered as described above, so that $[v_1]$ is a terminus of G, $[v_2]$ is a terminus of $G \setminus \{[v_1]\}$, and so on, then we shall have $B_{st} = 0$ when $s < t$, so B will be block lower triangular.

DEFINITION. Let G be a directed graph. The set of all matrices of type G will be denoted by Y_G.

Note that if G is strongly connected, then there are no restrictions placed on matrices of type G, so $Y_G = M_n(F)$.

LEMMA 1. *If G is a directed graph on n vertices, then Y_G is a subalgebra of $M_n(F)$.*

Proof. Clearly Y_G is closed under addition and scalar multiplication. Suppose $C = (C_{ij})$, $D = (D_{ij}) \in Y_G$. Then the (i, j) block of CD is $\sum_{u=1}^{r} C_{iu} D_{uj}$ (where r is the number of strong components of G). If this is nonzero, then $C_{iu} \neq 0$ and $D_{uj} \neq 0$ for some u. But then $[v_i] \to [v_u]$ and $[v_u] \to [v_j]$, so $[v_i] \to [v_j]$ by the transitivity of $\to$. Hence $CD \in Y_G$. ■

LEMMA 2. *Let $A = \operatorname{diag}(a_1, a_2, \dots, a_n)$ where $a_1, \dots, a_n$ are distinct and nonzero. Let X be an F-subalgebra of $M_n(F)$ containing A, and let S be a generating set for X. Then if $G(S)$ is strongly connected, $X = M_n(F)$.*

Proof. Let E_{st} be the $n \times n$ matrix with 1 in position (s, t) and zeros elsewhere. It will suffice to show that X contains all the matrices E_{st}. Since

$a_1, a_2, \ldots, a_n$ are distinct and nonzero, each E_{ss} is a polynomial in A and hence X contains E_{ss} for $s = 1, 2, \ldots, n$. Now choose any s, t with $s \neq t$. Since $G(S)$ is strongly connected, $s \to t$. So there exist $q \geqslant 2$, some $B_1, \ldots, B_{q-1} \in S$, and $s_1 = s, s_2, \ldots, s_q = t$ such that

$$z = b^{(1)}_{s_1 s_2} b^{(2)}_{s_2 s_3} \cdots b^{(q-1)}_{s_{q-1} s_q} \neq 0,$$

where $B_h = (b^{(h)}_{uv})$.

Note that $V = E_{s_1 s_1} B_1 E_{s_2 s_2} \cdots B_{q-1} E_{s_q s_q} \in X$. But $V = zE_{st}$. Hence $E_{st} \in X$, and the lemma is established. ■

We now state the main result of this paper.

THEOREM 1. *Let $A = \operatorname{diag}(a_1, \ldots, a_n) \in M_n(F)$, where $a_1, \ldots, a_n$ are distinct and nonzero. Let X be an F-subalgebra of $M_n(F)$ containing A, and let S be a generating set for X. Then X is determined up to permutation similarity in $M_n(F)$ by $G(S)$. More explicitly, X is similar via a permutation matrix to the algebra $Y_{G(S)}$.*

Proof. Relabel the vertices of $G(S)$ so that

$$[v_1] = \{1, 2, \ldots, k_1\},$$

$$[v_2] = \{k_1 + 1, k_1 + 2, \ldots, k_1 + k_2\}$$

$$\vdots$$

In terms of matrices, this amounts to carrying out a similarity via a permutation matrix. Note that $A \in Y_{G(S)} = Y$, say, and also $S \subseteq Y$. Hence $X \subseteq Y$, since, by Lemma 1, Y is an F-subalgebra.

For a block matrix $C = (C_{ij})$ we write $(C)_{st}$ to denote the matrix whose (s, t) block is C_{st} and all of whose other blocks are zero. Suppose $C = (C_{ij}) \in X$ and $C_{st} \neq 0$. Now $(I)_{ss}$ and $(I)_{tt} \in X$ (where I is the $n \times n$ identity matrix), since $A \in X$ and A has distinct eigenvalues, so

$$(C)_{st} = (I)_{ss} C (I)_{tt} \in X.$$

In particular $(U)_{ii} \in X$ for all $U \in S$.

Applying Lemma 2, we see that

$$\{(A)_{ii}\} \cup \{(U)_{ii} | U \in S\}$$

generates $M_{k_i}(F)$. Hence $(C)_{ii} \in X$ for all $C \in M_n(F)$ and $i = 1, 2, \ldots, r$. This completes the proof of the theorem if $r = 1$.

Suppose that $r > 1$ and that $[v_i] \neq [v_j]$ and $[v_i] \to [v_j]$. It suffices to show that $(C)_{ij} \in X$ for all $C \in M_n(F)$.

Suppose first that there exists $D \in X$ with $D_{ij} \neq 0$. Then for all $W, Z \in M_n(F)$,

$$(W)_{ii}(D)_{ij}(Z)_{jj} \in X.$$

Hence $(U)_{ij} \in X$ for all $U \in M_n(F)$. Hence we need only show that such a D exists. Since $[v_i] \to [v_j]$, there exist $m \geqslant 1$, $B_1, \ldots, B_{m-1} \in S$ and $i_1 = i, i_2, \ldots, i_m = j$ such that

$$(B_1)_{i_1 i_2} \neq 0, \ldots, \qquad (B_{m-1})_{i_{m-1} i_m} \neq 0.$$

But then $(U)_{i_1 i_2}, \ldots, (U)_{i_{m-1} i_m} \in X$ for all $U \in M_n(F)$. For a suitable choice of $U_1, \ldots, U_{m-1} \in M_n(F)$

$$D = (U_1)_{i_1 i_2}, \ldots, (U_{m-1})_{i_{m-1} i_m} \neq 0$$

and $D = (D)_{ij} \in X$. This completes the proof. ■

THEOREM 2. *Under the hypotheses of Theorem* 1, *the following are equivalent for* $n > 1$:

(1) X *is simple.*
(2) $X = M_n(F)$.
(3) $G(S)$ *is strongly connected.*

THEOREM 3. *Under the hypotheses of Theorem* 1, *the following are equivalent*:

(1) X *is semisimple.*
(2) $G(S)$ *is symmetric under* $\to$.

THEOREM 4. *Under the hypotheses of Theorem* 1, X *is the algebra generated by* A, B, *where* B *is the* $(0, 1)$ *matrix with* $b_{ii} = 1$ *for all* i, *and for* $i \neq j$, $b_{ij} = 1$ *if and only if* $i \to j$. *In particular* X *is two-generated.*

COROLLARY. *A is contained in only finitely many subalgebras of $M_n(F)$.*

EXAMPLE 1. The F-subalgebra of $M_n(F)$ formed by all matrices of the form

$$\begin{pmatrix} 0 & 0 \\ C & 0 \end{pmatrix}$$

where C is an $[n/2] \times [n/2]$ matrix (where $[\cdot]$ denotes the greatest-integer function) requires $[n/2]^2$ generators, since the product of every pair of its elements is zero. This contrasts greatly with the conclusions of Theorem 4.

EXAMPLE 2. Let F be an infinite field, and for each 3-tuple $a \in F^3$ which is not a scalar multiple of $(1, 1, 1)$, let

$$W_a = \operatorname{span}\{a, (1,1,1)\}.$$

Let Δ_a be the algebra of all matrices of the form

$$\begin{bmatrix} 0 & x_1 & y & z \\ 0 & 0 & x_2 & w \\ 0 & 0 & 0 & x_3 \\ 0 & 0 & 0 & 0 \end{bmatrix},$$

where $y, z, w \in F$ and $(x_1, x_2, x_3) \in W_a$.

Then there are infinitely many W_a's, all of which contain

$$\begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

So the corollary fails in general for nonderogatory matrices. However, see [7] for a result in this situation.

EXAMPLE 3. Let

$$A_1 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \qquad A_2 = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix},$$

$$S_1 = \{A_1, B\}, \qquad S_2 = \{A_2, B\}.$$

Then

$$[G(S_1)] = [G(S_2)] = \{[1],[2]\},$$

and in each case $[2] \to [1]$. However, the subalgebras of $M_2(F)$ generated by S_1, S_2 are not isomorphic. Thus Theorem 1 must be modified if we allow A to be singular. This situation is discussed below.

Assume that A is singular in Theorem 1, say $A = \operatorname{diag}[a_1, \ldots, a_n]$ with $a_1, \ldots, a_n$ distinct, and without loss of generality, $a_1 = 0$. It is straightforward to check that the conclusion of Theorem 1 holds as stated if $1 \to 1$ in $G(S)$. Suppose $1 \nrightarrow 1$ in $G(S)$. We may assume

$$[G(S)] = \{[1],[v_2],\ldots,[v_r]\},$$

where $[v_2] = \{2, \ldots, k_2 + 1\}$, $[v_3] = \{k_2 + 2, \ldots, k_2 + k_3 + 1\}$, etc. For each $U \in M_n(F)$ write $U = (U_{ij})$ in block form where the diagonal blocks U_{ii} are $k_i \times k_i$ and $k_1 = 1$. Let $U_2 = (U_{ij})_{2 \leqslant i,j \leqslant r}$ and $X_2 = \{U_2 \mid U \in X\}$. Note that X_2 contains A_2 and that its structure is determined by Theorem 1 applied to $S_2 = \{B_2 \mid B \in S\}$. In particular, using the notation of Theorem 1, $(U)_{ii} \in X$ for all $i \geqslant 1$ and all $U \in M_n(F)$.

Suppose $[1] \to [v_1]$ in $[G(S)]$, some $i > 1$. Then as in the proof of Theorem 1, $(U)_{1i} \in X$ for all $U \in M_n(F)$. Similarly, if $[v_j] \to [1]$ in $[G(S)]$, some $j > 1$, then $(U)_{j1} \in X$ for all $U \in M_n(F)$. Hence X consists of all block matrices $U = (U_{ij})$ subject to the conditions $U_2 \in X_2$ and $U_{1s} = 0$ if $[1] \nrightarrow [v_s]$, $s > 1$, and $U_{tl} = 0$ if $[v_t] \nrightarrow [1]$, $t > 1$, in $[G(S)]$.

We now consider spanning sets for X.

PROPOSITION. *Let X be a subalgebra of $M_n(F)$ containing $A = \operatorname{diag}(a_1, a_2, \ldots, a_n)$, where $a_1, a_2, \ldots, a_n$ are distinct and nonzero. Suppose X is generated by A, B. Then X is spanned over F by the monomials of the form*

$$A^i \qquad (i = 0, 1, \ldots, n-1),$$

$$A^{i_0} B A^{i_1} B \cdots B A^{i_{r-1}} B A^{i_r}$$

where $r \geqslant 1$, $i_0, i_1, \ldots, i_r$ are nonnegative integers, $i_0 \leqslant n-1$, $i_r \leqslant n-1$, and $i_1 + i_2 + \cdots + i_{r-1} \leqslant n-1$.

Proof. Let $\Gamma = \Gamma(B)$ be the directed graph associated with B. Note that X is spanned by the matrix units E_{ii} and those E_{uv} $(u \neq v)$ for which there exists a path from u to v in Γ. The elements E_{ii} lie in span$\{A^i \mid i = 0, 1, \ldots, n - 1\}$. Suppose u, v are given $(u \neq v)$ and that there exists a path

$$u = u_1 \to u_2 \to \cdots \to u_i \to u_{k+1} = v$$

of length k in Γ and no path of smaller length. We prove by induction on k that there exist nonnegative integers $i_1, i_2, \ldots, i_k$ with sum

$$i_1 + i_2 + \cdots + i_k \leqslant n - 1$$

such that the (u, v) entry of

$$BA^{i_1}B \cdots BA^{i_k}B \tag{1}$$

is nonzero. Let Y be the set of integers $w \neq u$ such that $b_{uw} \neq 0$ [where $B = (b_{ij})$]. Let m be the cardinality of Y. Note that there is a path in Γ from u_2 to v of length $k - 1$ and that if $u_2 \to y_3 \to \cdots \to y_k \to v$ is such a path, then none of the elements $y_3, \ldots, y_k, v$ lies in Y. Let A_1, B_1 be obtained from A, B by deleting row i and column i for all i in $Y \cup \{u\}$ except $i = u_2$. Then A_1, B_1 are $(n - m) \times (n - m)$ matrices, and by induction, there exist nonnegative integers $i_2, i_3, \ldots, i_k$ with $i_2 + i_3 + \cdots + i_k \leqslant n - m - 1$ such that

$$C_1 = B_1 A_1^{i_2} B_1 \cdots B_1 A_1^{i_k} B_1$$

has its (u_2, v) entry nonzero. But then

$$C = BA^{i_2}B \cdots BA^{i_k}B$$

has its (u_2, v) entry nonzero. Let $C = (c_{ij})$. The (u, v) entry of BA^iC is

$$\sum_{h=1}^{n} b_{uh} a_h^i c_{hv},$$

and this equals

$$\sum_{h \in Y} b_{uh} a_h^i c_{hv}. \tag{*}$$

Since Y has m elements and $b_{uh}c_{hv} \neq 0$ for $h = u_2$, a simple Vandermonde-determinant argument yields that there exists a nonnegative integer $i_1 \leqslant m - 1$

with the sum (*) nonzero. Since $i_1 + i_2 + \cdots + i_i < n - 1$, the assertion (1) follows. But now, since E_{uu}, E_{vv} lie in span$\{A^i \mid i = 0, 1, \ldots, n-1\}$, the proof of the proposition is complete. ■

COROLLARY 1. *Under the hypotheses of the proposition, X is spanned by the monomials in A, B of total degree at most $3n + k - 3$, where k is the maximum of the (shortest) distances between pairs of connected vertices u, v ($u \neq v$) in $\Gamma(B)$.*

In particular, since $k \leqslant n - 1$, we have

COROLLARY 2. *Under the same hypotheses, X is spanned by the monomials in A, B of total degree at most $4n - 4$.*

REMARK. The bound in Corollary 2 is of interest because it is linear in n. (Bounds available in the literature for general B are quadratic in n). The best possible bound is conjectured to be $2n - 2$. This arises for example when $X = M_n(F)$ and B has rank one or B is a monomial matrix. See Paz [9] and Laffey [8] for details.

THEOREM 5. *Let F be a field, and let A, B, C, D in $M_n(F)$ satisfy the following conditions:*

(i) *A has n distinct nonzero eigenvalues;*

(ii) *the algebra X generated by A, B is $M_n(F)$;*

(iii) *for all monomials $m(x, y)$ in the noncommuting indeterminants x, y, of total degree at most $8n - 7$,*

$$\operatorname{tr} m(A, B) = \operatorname{tr} m(C, D)$$

(*where* tr P *denotes the trace of* P).

Then there exists a nonsingular matrix T with $T^{-1}AT = C$, $T^{-1}BT = D$.

Proof. Let Y be the algebra generated by C, D. By the proposition, X has a basis U consisting of monomials $M(A, B)$, each of which has total degree at most $4n - 4$. We will first show that $V = \{M(C, D) \mid M(A, B) \in U\}$ is linearly independent. This implies that $\dim Y \geqslant \dim X$ and hence $Y = M_n(F)$ and V is a basis for Y.

We show that V is linearly independent by showing that if $M_1(C, D), \ldots, M_k(C, D)$ are monomials, each of total degree at most $4n - 4$, which are linearly dependent over F, then the monomials $M_1(A, B), \ldots, M_k(A, B)$ must also be linearly dependent.

Suppose $\sum_{i=1}^{k} a_i M_i(C, D) = 0$. Then for any $N(A, B)$ in the basis U, we have

$$\sum_{i=1}^{k} a_i M_i(C, D) N(C, D) = 0.$$

Condition (iii) then tells us that $\operatorname{tr}[\sum_{i=1}^{k} a_i M_i(A, B) N(A, B)] = 0$. But $X = M_n(F)$ and U is a basis for X, so we have $\operatorname{tr}[\sum_{i=1}^{k} a_i M_i(A, B) R] = 0$ for every $n \times n$ matrix R. Hence, $\sum_{i=1}^{k} a_i M_i(A, B) = 0$.

We now assert that if $M(A, B) \in U$ and

$$M(A, B) A = \sum a_N N(A, B),$$
$$N = N(A, B) \in U,$$

then

$$\begin{aligned} M(C, D) C &= \sum a_N N(C, D), \\ N &= N(A, B) \in U. \end{aligned} \tag{*}$$

For if $W(A, B) \in U$, then

$$\begin{aligned} 0 &= \operatorname{tr}\Big[M(A, B) A W(A, B) - \sum_N a_N N(A, B) W(A, B) \Big] \\ &= \operatorname{tr}\Big[M(C, D) C W(C, D) - \sum_N a_N N(C, D) W(C, D) \Big] \end{aligned}$$

[using (iii) and the fact that the monomials occurring have degree at most $8n - 7$], and this implies (*), since $Y = M_n(F)$ and $\{N(C, D) \mid N(A, B) \in U\}$ is a basis.

A similar argument yields that if

$$M(A, B) B = \sum_{N \in U} b_N N(A, B)$$

then

$$M(C, D) C = \sum_{N \in U} b_N N(C, D).$$

An inductive proof now yields that if $W(A, B)$ is any monomial, and if

$$M(A, B)W(A, B) = \sum_{N \in U} c_N N(A, B),$$

then

$$M(C, D)W(C, D) = \sum_{N \in U} c_N N(C, D). \qquad (\dagger)$$

We now define a map

$$f: X \to Y : p(A, B) \to p(C, D)$$

for all polynomials $p(x, y)$ in the noncommuting indeterminates x, y. Applying (†) to the monomials occurring in $p(A, B)$, we find that if

$$p(A, B) = \sum_{N \in U} d_N N(A, B)$$

then

$$p(C, D) = \sum_{N \in U} d_N N(C, D).$$

Hence f is well defined, and it is then clearly an algebra isomorphism. Since every algebra isomorphism of $M_n(F)$ is inner [1, Theorem (4.1)], it follows that there exists an invertible matrix T with $f(Q) = T^{-1}QT$ for all $Q \in X$. This completes the proof. ■

REMARK. The trace argument used in the proof of Theorem 5 is essentially that of Pearcy [10]. Taking F to be the complex field, $B = A^*$, and $D = C^*$, Theorem 5 gives a version of Specht's theorem on unitary similarity. (A standard argument yields that if $T^{-1}AT = B$ and $T^{-1}A^*T = B^*$, then there exists a unitary matrix S with $S^{-1}AS = B$.) For a most comprehensive discussion on unitary similarity including variants of Pearcy's result, see Helene Shapiro's survey paper [12]. The general problem of finding an algorithm to determine whether a given pair $A, B \in M_n(F)$ is simultaneously similar to a given pair $C, D \in M_n(F)$ has been solved by Friedland [5].

In conclusion, we note that several authors have considered the relationship between graphs and the structure of matrix subalgebras. References [2, 4, 6, 7, 10] give some typical results.

We wish to thank the referee for carefully reading the manuscript and making helpful suggestions which have greatly improved the exposition.

REFERENCES

1 A. A. Albert, *Structure of Algebras*, Amer. Math. Soc. Colloq. Publ. 24, 1961.

2 G. P. Barker, Automorphism groups of algebras of triangular matrices, *Linear Algebra Appl.* 121:207-215 (1989).

3 M. Behzad, G. Chartrand, and L. Lesniak-Foster, *Graphs and Digraphs*, Wadsworth, 1979.

4 G. M. Engel and H. Schneider, Cyclic and diagonal products on a matrix, *Linear Algebra Appl.* 7:301-335 (1973).

5 S. Friedland, Simultaneous similarity of matrices, *Adv. in Math.* 50:189-265 (1983).

6 T. J. Laffey, Simultaneous triangularization of a pair of matrices, *J. Algebra* 44:550-557 (1976).

7 T. J. Laffey, A note on matrix subalgebras containing a full Jordan block, *Linear Algebra Appl.* 37:187-189 (1981).

8 T. J. Laffey, Simultaneous reduction of sets of matrices under similarity, *Linear Algebra Appl.* 84:123-138 (1986).

9 A. Paz, An application of the Cayley-Hamilton theorem to matrix polynomials in several variables, *Linear and Multilinear Algebra* 15:161-170 (1984).

10 C. Pearcy, A complete set of unitary invariants for operators generating W^*-algebras of type I, *Pacific J. Math.* 12:1405-1416 (1962).

11 H. Schneider, The concepts of irreducibility and full indecomposability in the works of Frobenius, König and Markov, *Linear Algebra Appl.* 18:139-162 (1973).

12 H. Shapiro, A survey of canonical forms and invariants for unitary similarity, *Linear Algebra Appl.* 147:101-167 (1991).

Received 28 April 1990; final manuscript accepted 8 May 1990